☑ PLEASE RETURN TO

OFFICE OL/P&PS

NAME

TUBE STATION

ROOM NO. AND BUILDING

Project CRAFT (WANG) File

FUNCTIONAL REQUIREMENTS:

A. Word Processing

1. Text Subdivisions
2. Edit
3. Search
4. Format
5. Pagination

B. Electronic Mail/Message Processing

1. Distribution List
2. Multi-point distribution
3. Index
4. Schedule
5. Confirmation

C. Document Storage and Retrieval

1. Retrieve criteria
2. Retrieve logic
3. Filing
4. Deletion
5. Paging
6.

D. Data Management

1. Structured Input
2. Validation
3. Retrieval logic
4. Reporting
5. Programs

E. General Programability

F. Ease of Use

1. Prompts
2. User - defined prompts

G. System Commands

1. User - defined functions
2. List
3. Print
4. Rename
5. Copy
6. Move
7. Delete
8. Sort

H. Staff Communications System (SCS) Interface

1. Receive messages from SCS
2. Forwarding messages to SCS

I. Electrical Interface Specifications

1. Electrical
2. Code
3. Protocols

J. Security Requirements

1. Need-to-know safeguards
2. System Security

   a. Access Control
   b. Security monitor Audit Trail

3. Prevention of unauthorized user penetration
4. Data security

   a. Classification
   b. Encryption
   c. Transfer
   d. Storage

5. Operating System Security

   a. Audit trail
   b. Allow for disconnection

6. Hardware Security

   a. TEMPEST
   b. Magnetic Storage easily removed
   c. Non-removable must be volatile
   d. Printers have cartridge-type ribbons
   e. Provision for add-on
   f. Independent real-time clock
   g. Capacity to detect configuration change

7. Emergency Destruction

   a. Hand-held magnet
   b. Degaussing
   c. Physical destruction
   d. Sufficient damage

K. System Reliability

   1. Failsafe - failsoft features
   2. Failure detection function

L. Equipment Redundancy - 99% Reliability

M. System Reconfiguration

N. Physical Constraints

   1. Space allocations

      a. Small station
      b. Medium station
      c. Large station

   2. Electrical power
   3. Environmental factors

CRAFT PRELIMINARY REQUIREMENTS DEFINITION

1. INTRODUCTION

This paper documents the initial analysis of the requirements for Project CRAFT (Clandestine Records Applications Field Terminal). The introduction to the paper establishes a context for the study by first reviewing the CRAFT project itself, beginning with a project overview, followed by a discussion of the project objectives, then a review of the project chronology. Next is a description of the study, first outlining its purpose and scope, its methodology, and finally its organization.

1.1 CRAFT Project

1.1.1 Project Overview

The CRAFT project evolves from the serious need to improve information security in the Directorate of Operations field stations. [redacted] DO field facilities have had to "burn out" in the past 24 months because of terrorist attack or the instability of the host government. Clearly, our field stations require the increased safeguards which would result from the storage of information in a form more protected than paper files. Ultimately, information in the field should be protected by a system that requires decryption to translate the information into readable form. Further, information stored at DO field stations must be capable of being destroyed in a fraction of the time that present methods require. The destruction time of field information should be measured in minutes, not in hours as is the case today.

25X1

1.1.2 Project Objectives

The primary objective of the CRAFT project is to improve the security of field record holdings. Additional objectives are to provide the field officers with more information, in a more timely manner and in a better form, to hasten their work.

The approach chosen to meet these objectives is to introduce automated data processing (ADP) equipment and techniques into the field station environment. Efforts will focus on combining electronic storage and data processing capabilities with secure data communications to provide an integrated system for field station information security and management. It is envisioned that a standard field information management system can be developed, and tailored as necessary, to meet individual station requirements. This system must provide a capability to connect with the Agency Staff Communications System (SCS) to facilitate information flow in and out of the station in totally electronic (paperless) form.

The introduction of ADP technology in the field will also permit growth of two additional capabilities for increased data security. The first capability is the total encryption of all information electronically stored in the field. The second capability is the option for the removal of all sensitive information from high-threat areas overseas. As high quality communications circuits become available, field information will be removed to Headquarters-based systems, and will be accessible from the field via a high-speed data link.

Improved information security in day-to-day operations will be achieved through the implementation of rigorous automated access controls (sign-on procedures and passwords) that will enhance information compartmentation. Audit trails in larger installations will make it possible to track information flow and will provide a mechanism for damage assessment. Those documents that are not stored in electronic form will be reduced to microfiche, which can also be managed in a manner more secure than can paper.

Automated information handling should also materially aid the case officers in the performance of their operational missions of recruiting and handling agents by providing them with the capability to rapidly access, collate, compare, and display information relating to operational matters. This capability should dramatically reduce the amount of time that case officers must spend in handling correspondence and in searching for needed information from paper files. Thus, case officers will be allowed to concentrate their efforts on operational pursuits. They should be able to react more quickly to fast moving situations to meet critical reporting or target analysis deadlines.

The automation of field records will include a mechanism for efficient and complete reconstitution of a station's files after a "burn out" by storing electronic (back-up) copies at Headquarters. In today's environment, the process of reconstitution, if possible at all, is time-consuming and labor-intensive.

OGC

The enhanced control of classified information and the assurance against loss to unfriendly personnel, coupled with the increased effectiveness that will be provided to all field officers, will provide significant benefits. Without this aggressive program to enhance the protection of field information, the vulnerability of our information during crisis situations will remain high, and unacceptable dangers will persist with more possible compromises which might result in a loss of station records and, very possibly, of human life.

OGC

1.1.3 Project Chronology

The CRAFT project was initiated early in 1977 when the Deputy Director for Operations approved, in principle, the phased automation of operational and administrative record systems at DO field stations. In July 1978, IMS officers were sent to field stations in EUR, AF, and NE Divisions to make an initial evaluation of CRAFT viability. Later that year, a decision was made to implement an automated correspondence and records system in [redacted] branch locations, to serve as a domestic 25X1 testbed of CRAFT technology before deployment overseas. Concurrently, a CRAFT System Development Center was established at Headquarters to test and evaluate equipment being considered for field use. In May 1979, a testbed for TEMPEST word processing equipment was installed in [redacted] 25X1 [redacted] During 1980, additional 25X1 CRAFT field surveys were completed by division Records Management Officers when they visited their stations. In January 1981, the biographic index search capability in [redacted] testbed became 25X1 operational and in March 1981 a word processor, with a paper tape interface [redacted] was installed in [redacted] Most 25X1 recently the CRAFT project office completed its analysis of field record holdings and Headquarters questionnaires, activities which led to the preparation of this Preliminary Requirements Study.

1.2 Preliminary Requirements Study

1.2.1 Study Purpose and Scope

The purpose of this study is to initiate the process of defining the particular requirements which must be satisfied by the CRAFT project to solve the problems and achieve the objectives previously outlined. The requirements detailed herein reflect actual testbed experience and an analysis of interviews (including the completion of a records survey questionnaire) with Headquarters personnel who have had recent field experience. This analysis will first examine the information management needs reflected in the current duties and functions of station personnel and in the record holdings currently supporting station operations; then it will outline the requirements which ADP technclogy must satisfy in order to provide automation assistance in station operations so as to effect the desired improvements in data security and duty performance.

The findings described in this paper constitute a preliminary requirements definition. This definition will be updated in a subsequent analysis of on-site surveys in the field, and will result in the publication of a Requirements Update

Document. That document will, in turn, be updated as a result of further post-survey analyses and additional requirements study. This will result in the publication of the final requirements paper, the Baseline Requirements Document.

1.2.2 Study Methodclogy

Members of the CRAFT Project Office interviewed case officers, operations support assistants, intelligence analysts, secretaries, and other personnel with recent experience in selected field stations to facilitate a preliminary definition of the stations' information management requirements, and to determine the form and function of field record holdings. Questionnaires were filled out to document the information flow and storage and retrieval procedures, so as to permit the specification and design of automated support equipment and techniques which would provide the particular automated services required by station personnel in the performance of their operational duties. A questionnaire was completed for each type of file maintained in the station. The questionnaire was designed to describe who uses the file and how often, the purpose of the file, and how long the information is retained. An example of the questionnaire form is shown in Appendix A.

When the interviews were completed, the questionnaires were sorted according to file type, and a comparison of the frequency of use, search method, retention, and disposition of the files was calculated.

An additional part of the requirements analysis was to develop a profile of each field station based on data held in the IMS Records Management Branch, the Office of Security, the Office of Communications, and various other sources. This data is related to the linear footage of records and burn times at each station. This profile, shown in Appendix B, is the technical basis for priority ranking of DO field stations for CRAFT installations.

1.2.3 Study Organization

The study begins by examining the current field station environment (Section 2), first in terms of station personnel duties and functions (Section 2.1), then in terms of the files in use (Section 2.2). The study then delineates the particular ADP functions which must be provided and specifies the requirements which must be met by the implementation technology (Section 3). This is followed by an articulation of the security requirements (Section 4). Section 5 addresses the stringent performance standards which must be met by the ADP equipment; Section 6 examines system administration; and finally, Section 7 documents the installation requirements.

2. FIELD STATION ENVIRONMENT

2.1 Station Personnel, Duties, and Functions

Although stations vary greatly in size, [redacted] 25X1
[redacted] the functional positions outlined in this section 25X1
are common to all field stations. Personnel usually include a
[redacted] 25X1

Next 1 Page(s) In Document Denied

2.2 Station Files

The types of files found in the field do not vary greatly from station to station. Each station maintains files that are a subset of the listing in Appendix C. These files, which vary in size and scope in relation to the station's activity, are maintained in compliance with [redacted] Disposition of Records. The manner in which files are used, the need for immediate retrieval, and the frequency of use was determined through interviews with a cross-section of DO personnel. The profile of the interviewees is shown in Appendix D.

At a minimum, each station maintains a central chrono file of recent correspondence and several other necessary files. In order to be operationally effective, the station requires a [redacted]

3.1 Word Processsing

One of the most labor-intensive and, consequently, resource-consuming activities in any station is typing. While the formats of documents created in the field are not complex, any automated system must provide extensive capability in this area. The following word processing functions are required.

1. Text Subdivisions - The user must be able to logically isolate a character, word, sentence, line, paragraph, or specified section in a document for edit by the system.

2. Edit - The system must allow any subdivision to be inserted, deleted, changed, moved or copied to or from any location in the document.

3. Search - The system must allow any string of characters to be located and changed in every occurrence within a document.

4. Formats - The system must allow commonly used phrases or formats to be stored and recalled when desired.

5. Paginaticn - The system must automatically title and number pages as specified.

3.2 Electronic Mail/Message Processing

To provide for the electronic receipt, review, and dissemination of incoming messages, and the rapid and controlled coordination and release of cables and reports, a facility that allows a user to send a document to another person is essential. The basic capabilities required to perform this function are as follows:

1. Distribution List - A user must be able to create and update one or more lists of persons who would receive any documents routed by a specific list.

2. Multi-Point Distribution - Distribution of documents of broad interest to a large group or class of individuals must be performed by a single indicator to avoid the necessity of building and maintaining large lists.

3. Index - As mail is routed to a user, basic information such as the sender's name, date and time sent, and title must be placed in an index so all mail may be quickly reviewed without retrieving and reading entire documents.

4. Schedule - The system must provide for both scheduled periodic distribution of mail as well as non-scheduled priority distribution at the user's direction.

5. Confirmation - A recipient must be able to confirm delivery if required, as in the case of high priority messages.

3.3 Document Storage and Retrieval

With all records in a station committed to electronic form, rapid and simple techniques for retrieving documents are all important. The following capabilities are required to allow ready access to all records, ensure ease of reading, and provide basic records maintenance functions.

1. Retrieve Criteria - The user must be able to specify any portion of a document for retrieval, such as date, subject, or originator.

2. Retrieval Logic - In a single retrieval request the user must be able to specify a number of search strategies, using Boolean logic, on various parts of a document.

3. Filing - The system must allow a document to be logically placed into as many files as requested.

4. Deletion - The system must allow a subset of the documents to be removed from the system by a single criteria, such as date or subject.

5. Paging - After a document has been retrieved, the user must be able to freely page forward and backward through the document.

6. Annotation - Some facility must be available to append comments and action requests to any document.

3.4 Data Management

Many of the records kept in the field are not in a formal document format. [redacted] are examples of information held by a station that could easily be stored and maintained in an automated system. To make such a record management tool usable to field personnel, the following characteristics must be present.

25X1

1. Structured Input - The input of data into the system must be through a format, as familiar as paper forms, displayed on the terminal screen.

2. Validation - The system must be able to monitor input and indicate when data is entered incorrectly.

3. Retrieval Logic - The system must use the same search techniques as for document retrieval.

4. Reporting - The user must be able to display any combination of data from the records in any format desired.

5. Programs - There must be a facility for permanently storing cften-used reports and retrievals.

3.5 General Programability

Because unique requirements, which cannot be met by vendor supplied software, invariably surface, a general purpose, high level language programming capability is needed to develop solutions in this area. Unrestricted use of this facility will be limited to Headquarters data processing professionals. The power and complexity of such a tool would make control and training, for its use in the field, extremely difficult.

3.6 Ease of Use

Because the training and guidance provided by records management personnel at Headquarters are not readily available to field personnel, any automated records system deployed to the field must require only the barest minimum of user training. The system should also provide assistance in identifying problem situations and monitoring normal operations. To ensure this, all system functions outlined in this section must be available to the user in both forms described below.

1. Prompts - The user must be allowed to set up any type of work activity offered by the system by simply answering a series of prompting questions. These questions must be phrased in non-technical terms and require a single answer before the next informative prompt is given.

2. User-Defined Prompts - For more knowledgeable users, the system must allow user-defined prompts which provide for the abbreviation of user steps and the rapid change from one function to another.

3.7 System Commands

All computer systems have a collection of basic functions which are usually performed in the background (unseen) without interaction with the user; however, these operations should also be available for explicit execution by personnel responsible for system administration. (This execution mode will be restricted to personnel with appropriate training and experience.) A list of these functions follows.

1. User-Defined Function - Similar to the user-defined prompts, this function tailors the system to perform well-defined and often-used activities. (With this capability, a group of system commands can be executed by entering a single phrase or short series of key strokes.)

2. List - Data such as document name, document type, author, creation date, and revision date must be available on request, sorted in any order specified. Similar information on data files and user-defined functions will also be available.

3. Print - This function will queue documents or data to a local printer.

4. Rename - This function will change the name of any document, data file, or user function.

5. Copy - An identical copy of a document, data file, or user function will be created as specified on the same physical storage device or any other accessible device.

6. Move - A copy of a document, data file, or user function will be created where requested and the original deleted.

7. Delete - Any document, data file, or user-defined function will be completely removed from the system.

8. Sort - This function will sort requested data by single or multiple keys and arrange the data in ascending or descending order.

4. SECURITY REQUIREMENTS

The following requirements are a basic outline of the security considerations directly applicable to automated field records systems. For the detailed security specificcations the reader must consult the ISSG document "Security Requirements for Automated Information Systems Located in Overseas Installations".

4.1 Need-to-Know Safeguards

Only staff emplcyees who possess an established need-to-know, as determined by the Chief of Station, will be allowed access to the CRAFT equipment. If cryptographic equipment or material is installed in the CRAFT facility, appropriate cryptographic clearances will be required. Access to the approved storage area in which data and program storage media are maintained will be restricted to staff employees.

4.2 System Security

4.2.1 Access Control

Each user will be required to gain access to the system through a unique identifier and matching password. In addition, user access to any data file will have to be controlled by a unique subsystem password; the password will be authenticated by the security system each time the user desires to retrieve and/or modify data. The password, which must be at least six characters in length, cannot be printed or displayed at any terminal and will hold the same classification as the data which it protects.

There must be a provision for the secure storage of passwords in the system. Through a function available only to the System Security Officer, there must be a means of adding, deleting, and/or changing authorization profiles. User subsystem passwords must be changed:

1. Immediately following any suspected security compromise;

2. When it is determined that a user no longer requires access to the system; or

3. Every six months, unless more frequent changes are required for stations in high threat areas.

Page Denied

Next 2 Page(s) In Document Denied

4.3 Data Security

4.3.1 Classification

Each file in the system will be assigned a security classification which will reflect the highest classification found within the file. The system must not store documents until a recognizable security classification is provided. Security markings will be UNCLASSIFIED, CONFIDENTIAL, SECRET, SECRET RYBAT, SECRET PRESCRIBED AND LIMITED, TOP SECRET, with collateral security classifications, and Chief of Station EYES ONLY. The classification must be placed on appropriate VDU's and on printed output.

The system must label all information output with its associated markings at the top and bottom of each page (in compliance with [redacted] This will apply to all output media including workstations and hard-copy output devices. However, the system must also have the ability to inhibit the labeling of output. There must also be a provision for the System Security Officer to modify the markings for files, records within files, and fields within records.

25X1

4.3.2 Encryption

Sensitive files will be identified and consideration given to the possibility of storing the data in encrypted form. Provision must be made for the ultimate addition of a device or algorithm that will encrypt all data held on the storage media.

4.3.3 Transfer

Communications between elements of the CRAFT System which are in separate locations and not directly connected by shielded cable will be via removable storage media (e.g. diskette).

The transportation of classified data between Headquarters and the field will be in accordance with established Agency procedures issued for the shipment and handling of classified and sensitive information.

4.3.4 Storage

All demountable data and program storage media, when not in use, will be placed in an approved Class 5 security container. These security containers will be located within the station vault or secure area. The security containers may remain in the ADP facility if the facility meets the standards established for a vault or secure area.

4.4 Operating System Security

The information processing functions which use an operating system must:

1. Incorporate an audit trail in all input/output functions related to all resources (as noted in [redacted]

25X1

2. Allow for the disconnection, by software control, of any workstation without degrading overall operations or security.

4.5 Hardware Security

Hardware components destined for installation in the field must meet the following requirements:

1. All equipment must be TEMPEST certified.

2. All magnetic storage media must be easily removed.

3. Any non-removable, internal memory must be volatile (completely erased when the device is turned off).

4. All printers must use cartridge-type printer ribbons that can be easily removed.

5. There must be a provision for later addition of a device or algorithm to encrypt data that is stored or transmitted.

6. The system must have a real-time clock with an independent power source.

7. The system must have the capacity to detect any change of status in the hardware configuration, i.e.,

the ability to detect the connection or disconnection of a device. [redacted]

25X1

25X1

Page Denied

4.7 System Security Officer Responsibility

The Chief of Station, in coordination with the Headquarters component, will designate a subordinate to act as the local System Security Officer. The System Security Officer will establish and implement a formal system security program to ensure compliance with the requirements established herein. In addition, the local System Security Officer will be charged with the operation of the system security software. This will include updating profiles in the sign-on function and monitoring the audit trail, as noted in Sections [redacted]

25X1

4.8 Physical Security

Physical security will be in compliance with appropriate regulations regarding the proper handling and storage of classified information. All CRAFT hardware and other equipment associated with it must be within Agency controlled space, in an interior room when possible.

When remote terminals are used, they will be in Agency controlled space and will have a logical disconnect when the system is secured at close of business. All equipment will be situated so that a 10-foot separation is provided between transmitting and receiving devices in the classified and unclassified modes. The maintenance of the equipment will be performed by either cleared U.S. Government personnel or by U.S. citizens in the presence of station personnel.

5. SYSTEM RELIABILITY REQUIREMENTS

5.1 Software Reliability

Because frequent or prolonged system failures would intolerably degrade the effectiveness of CRAFT, the system must be highly reliable, fault tolerant, with fast recovery and/or reconfiguration. In essence, a high degree of reliability is the most fundamental requirement for CRAFT hardware and software. A system failure, for the purpose of CRAFT requirements, is defined as the loss of a major function or workstation to any single user.

The system will be considered to be in a degraded state if there is a drop below 100% of normal operating capacity. Recovery should be system initiated or, at most, require minimal user intervention. User interaction with the system functions must be via a menu format in order to provide the greatest possible user error-protection. Further protection will be provided by disabling the keyboard (lock-out) while the system processes user commands. Interaction with word processing and data processing functions must be in response to system prompts. Error detection logic must be capable of generating interrupts to cease program operations that might lead to system errors. To meet the stringent software reliability requirements, the CRAFT system must be designed with:

1. Failsafe-failsoft features to minimize the impact of system or subsystem failures.

2. A failure detection function to provide user-error protection and to facilitate a graceful degradation and quick recovery.

5.2 Equipment Redundancy

There must be full redundancy of all hardware components to provide no less than 99% reliability. To meet this requirement, one or more backup configurations will be installed at each facility. The redundant equipment must be operating and readily available to the user by being incorporated into the standard CRAFT configuration. The standard configuration is defined as the necessary equipment to provide each field station with its basic requirements at least 99% of the time. Hence, the standard configuration will be dependent upon the unique station size and workload and will vary from station to station. In all cases, there must be an adequate backup capability.

5.3 System Reconfiguration

Following a need to take a particular device off-line, there must be a provision for the system to be reconfigured which will allow the system to continue operating in a slightly degraded, but reliable, condition. To meet this requirement, the devices must be of the component variety that can be mixed or deleted without causing a system failure. Thus, the system must be able to accept the transfer or deletion of devices.

6. SYSTEM ADMINISTRATION

6.1 System Management

For the purpose of this requirements study, it is necessary to identify the essential functions of local system management. The ultimate responsibility for the management of each CRAFT installation rests within the CRAFT Project Office. However, each field installation will have a station member who is designated to be the local system manager by the COS. Each local system manager will be responsible for the following functions:

1. Ensuring that adequate consumables (e.g., printer ribbons, etc.) and disk packs are on hand.

2. Conducting local familiarization and training for new station members.

3. Monitoring the equipment status and notifying Headquarters when there are significant equipment failures.

4. Managing the backup procedures to provide adequate records for reconstitution.

5. Establishing the standard hours of operation.

The duty of system management should not require more than a few hours additional time each week. To monitor the system, the local system manager may choose to delegate some of the routine functions of the system management.

6.2 User Training

The majority of user training will be conducted at Headquarters. Individuals destined for PCS assignments in the field will be scheduled for user training prior to their departure. When possible, CRAFT officers on TDY visits to field stations will provide refresher training and brief the system manager on new developments. Since the system will be menu-driven, the majority of training will be in word processing functions and basic data retrieval. This training can be accomplished within a few days.

6.3 Data Destruction

Data destruction is the responsibility of the System Security Officer (who will proceed as directed in Section [redacted]. 25X1

6.4 Backup and Reconstitution

The backup of field records is the responsibility of the local system manager. The frequency of this procedure will be established by the CRAFT Project Office. Following a complete records destruction, it will normally be necessary to restore the station's records holdings. Headquarters will provide the station with the current backup copy of the station's latest files.

7. INSTALLATION REQUIREMENTS

7.1 Physical Constraints

Physical constraints imposed by both the Office of Security and the Communications Security Division (COMSEC) of the Office of Communications will affect installation of the data processing equipment associated with the CRAFT program. These constraints are imposed primarily because the data which is now stored in safe-keeping devices in a station will be contained within the system on magnetic media (either on diskettes or on rigid disk packs). The physical constraints are required to enhance the protection of this data by denying, insofar as possible, access by hostile entities to the CRAFT system or its components.

The installation of a CRAFT system will require the continual presence of American citizen security guards at the building entrance. All areas in the station must have both volumetric alarms and door/window contact alarms monitored at a central guard station. These alarms will serve to alert the guard force to possible penetration of the space where the systems are located. The security requirements necessary to

Page Denied

protect the data against unauthorized access without regard to the physical space alarms are addressed in Section 4.

[redacted]

[redacted]

25X1

7.1.1 Space Allocation

Equipment selected for use in CRAFT systems must be modular, thus permitting flexibility in sizing to support varying station requirements. The space and weight requirements described below will vary somewhat, but they do represent an acceptable "rule of thumb".

25X1

7.1.2 Electrical Power

CRAFT equipment must operate on 240volt/50Hz power. The equipment should be designed for the office environment in the sense that it need only be unpacked, hooked up, and be operable in the local environment.

[redacted] 25X1

[redacted] The necessary modifications must be performed prior to 25X1 the installation and operation of each CRAFT system.

7.1.3 Environmental Factors

CRAFT data processing equipment must be designed for use in a nominal office environment which normally does not require heating, ventilation, air-conditioning (HVAC) enhancement. Generally, operating environments are between 50-90 degrees Fahrenheit, with non-condensing humidity of 20% to 80% (although the reccommended relative humidity is 35% to 65%, non-condensing). In a normal controlled office area [redacted] [redacted] the CRAFT system must be operable without enhancement. In those station locations where office environments normally fall outside the above-noted operating ranges, appropriate GFE HVAC system supplements will be provided to correct the problem.

Next 2 Page(s) In Document Denied

7.2.2 Accessibility

Field operations do not conform to any timetable, therefore information must be accessible to station personnel whenever requested. To meet this requirement, the system must be readily available both physically and logically.

To prevent the need of accessing a number of offices, all equipment necessary for data retrieval should be located in work areas normally accessible to the operations personnel who would require this information. Otherwise, valuable time would be lost while additional personnel were called in to the station to assist in readying the system for use.

In addition to physical access, the startup procedure must be simple enough for all personnel to be able to turn the system on without technical assistance. Extensive knowledge of which components comprise a minimum working system, how the equipment must be powered on, or what commands must be given to ready a work station for use should not be required.